

Notice of Allowability	Application No.	Applicant(s)	
	09/596,652	BERSON ET AL.	
	Examiner	Art Unit	
	Grigory Gurshman	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 12/05/2005.
2. ☒ The allowed claim(s) is/are 1-3, 5-15, 17-22.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 - * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. <input type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other _____ |
|---|---|

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Daniel B. Curtis on 12/20/2005.

The application has been amended as follows:

Claim 1: A method for providing a cryptographic service utilizing a server on a network, comprising:

- (a) identifying, by the server, a client utilizing the network;
- (b) generating a tunnel on the network using a first key;
- (c) receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair;
- (d) receiving a performance speed specification for the cryptographic service; and
- (e) performing the cryptographic service at the server for the client, responsive to the performance speed specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

Art Unit: 2132

Claim 13: A computer program embodied on a computer readable medium for providing a cryptographic service utilizing a server on a network, comprising:

- (a) a code segment for identifying, by the server, a client utilizing the network;
- (b) a code segment for generating a tunnel on the network using a first key;
- (c) a code segment for receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair;
- (d) a code segment for receiving a performance speed specification for the cryptographic service; and
- (e) a code segment for performing the cryptographic service at the server for the client, responsive to the performance speed specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

Claim 20: A system for providing a cryptographic service utilizing a server on a network, comprising:

- (a) computer logic for identifying, by the server, a client utilizing the network;
- (b) computer logic for generating a tunnel on the network using a first key;
- (c) computer logic for receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair;
- (d) computer logic for receiving a performance speed specification for the cryptographic service; and
- (e) computer logic for performing the cryptographic service at the server for the client, responsive to the performance speed specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

2. The support for the amendment is found at page 22, lines 1-6.

Allowable Subject Matter

3. Claims 1-3, 5-15, 17-22 are allowed.

4. The following is an examiner's statement of reasons for allowance:

4.1 The rejection of claim 20 under 35 USC 101 has been overcome by examiner's amendment.

4.2 Referring to the instant claims, McGravey discloses a method for delegating authority in a public key authentication environment from a client to a server machine or process, in order that the server machine or process can then securely access resources and securely perform tasks on behalf of the client (see abstract).

McGravey shows in Fig. 6 that the client sends an initial request at 601, comprising a nonce (nonce1) and a request for the server's certificate. The server forwards or tunnels all the client information received from the client during the handshaking process on to the private key system as shown at 602. The private key system now has the nonce1 (from the client), and the original request from the client. The private key system responds 603 by sending a signed nonce1, a nonce2, and the private key system's certificate (identified in FIG. 6 as the security certificate) to the server. The server then forwards 604 this information to the client. The client then responds 605 by sending a signed nonce2 and the client certificate to the server. The server forwards 606 or tunnels this information to the private key system.

4.3 McGravey, however does not teach or suggest using the "speed specification

Art Unit: 2132

for the cryptographic service". Furthermore, McGravey does not teach receiving the encrypted client's private key at the server and performing the cryptographic service by the server using the decrypted client's private key of a public key pair.

4.4 Referring to the instant claims, Dolan discloses a public key communication system (see Fig. 1). Dolan teaches a data communications system is described in which messages are processed using public key cryptography with a private key unique to one or more users (150). The server (130) has access to, the private key for each, user in encrypted form only. The private key is encrypted with a key encrypting key and each security device (120) comprises means for storing or generating the key encrypting key and providing the key encrypting key to the server (130). The server comprises secure means (360) to retrieve the encrypted private key for the user, decrypt the private key using the key encrypting key, perform the public key processing using the decrypted private key. However, Dolan does not teach using the "speed specification for the cryptographic service" requested by the client. Therefore, the combination of McGravey and Dolan does not render the instant claims obvious.

5. In view of the reasons presented herein claims 1-3, 5-15, 17-22 are in condition for allowance.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

Art Unit: 2132

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

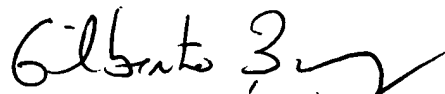
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



GG
December 21, 2005

Grigory Gurshman
Examiner
Art Unit 2132



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100